No. 06-1602

In the Supreme Court of the United States

CHRISTOPHER ANDREW PHILLIPS, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

PAUL D. CLEMENT
Solicitor General
Counsel of Record

ALICE S. FISHER
Assistant Attorney General

MICHAEL A. ROTKER
Attorney

Department of Justice
Washington, D.C. 20530-0001
(202) 514-2217

QUESTION PRESENTED

Whether the district court committed reversible plain error by instructing the jury that it could convict petitioner for knowingly transmitting a program to a protected computer, in violation of 18 U.S.C. 1030(a)(5)(A)(i) (Supp. IV 2004), where the indictment charged that petitioner intentionally accessed a protected computer without authorization, in violation of 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004).

TABLE OF CONTENTS

Page

Opinion below 1
Jurisdiction 1
Statement 1
Argument 8
Conclusion 15

TABLE OF AUTHORITIES

Cases:

Almendarez-Torres v. *United States*, 523 U.S. 224 (1998) 9
Chapman v. *California*, 386 U.S. 18 (1967) 11
Hamling v. *United States*, 418 U.S. 87 (1974) 10
Johnson v. *United States*, 520 U.S. 461 (1997) 7, 9, 13, 14
Murphy v. *United States*, 546 U.S. 1097 (2006) 9
Neder v. *United States*, 527 U.S. 1 (1999) 11
Stirone v. *United States*, 361 U.S. 212 (1960) 10, 11
United States v. *Brown*, 400 F.3d 1242 (10th Cir. 2005) 14
United States v. *Cotton*:
535 U.S. 625 (2002) 9, 12, 13, 14
261 F.3d 397 (4th Cir. 2001), rev'd, 535 U.S. 625 (2002) 12, 13
United States v. *Floresca*, 38 F.3d 706 (4th Cir. 1994) 12, 13
United States v. *Miller*, 471 U.S. 130 (1985) 9

Cases—Continued: Page

United States v. *Murphy*, 406 F.3d 857 (7th Cir. 2005), cert. denied, 546 U.S. 1097 (2006) 13
United States v. *Thomas*, 274 F.3d 655 (2d Cir. 2001) ... 12

Constitution and statutes:

U.S. Const.:
Art. I, § 10, Cl. 1 (Ex Post Facto Clause) 6
Amend. V (Grand Jury Clause) 9
18 U.S.C. 1028(a)(6) (Supp. IV 2004) 4
18 U.S.C. 1029(a)(3) 4
18 U.S.C. 1030(a)(5) (2000 & Supp. IV 2004) 6, 8
18 U.S.C. 1030(a)(5)(A)(i) (Supp. IV 2004) 6, 10
18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004) 1, 4, 6, 7, 8, 10

Miscellaneous:

11th Cir. Pattern Jury Instructions–Criminal Cases (2003) 6
4 Wayne R. LaFave et al., *Criminal Procedure* (2d ed. 1999) 10, 11

In the Supreme Court of the United States

No. 06-1602

CHRISTOPHER ANDREW PHILLIPS, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINION BELOW

The opinion of the court of appeals (Pet. App. 1-17) is reported at 477 F.3d 215.

JURISDICTION

The judgment of the court of appeals was entered on January 24, 2007. A petition for rehearing was denied on March 1, 2007 (Pet. App. 29-30). The petition for a writ of certiorari was filed on May 30, 2007. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a jury trial in the United States District Court for the Western District of Texas, petitioner was convicted of intentionally accessing a protected computer without authorization and recklessly causing damage, in violation of 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV

2004). He was sentenced to five years of probation, five hundred hours of community service, and restitution of $170,056. Pet. App. 19, 26. The court of appeals affirmed. *Id.* at 1-17.

1. Petitioner became a student at the University of Texas at Austin (UT) in 2001. Despite signing UT's "acceptable use" computer policy, in which he agreed not to perform port scans using his university computer account,[1] petitioner used various programs designed to scan computer networks and steal encrypted data and passwords. He broke into hundreds of computers, including machines belonging to other UT students, private businesses, United States Government agencies, and the British Armed Services webserver. Petitioner thereby obtained a substantial amount of personal and proprietary data, such as credit card numbers, bank account information, student financial aid statements, birth records, passwords, and Social Security numbers. Pet. App. 2; Gov't C.A. Br. 4-5.

Petitioner's port scanning was detected by UT's Information Security Office (ISO), which warned him on three separate occasions to stop trying to breach the security of computer systems. Despite those warnings, petitioner continued to scan and infiltrate computers inside and outside the UT system, adding to his data-

[1] "Port scanning is a technique used by computer hackers by which an individual sends requests via a worm or other program to various networked computer ports in an effort to ascertain whether particular machines have vulnerabilities that would leave them susceptible to external intrusion. Often used as an initial step in launching an attack on another computer or transmitting a virus, port scanning is a relatively unsophisticated, but highly effective, reconnaissance method, likened at trial by UT's information technology chief as the electronic equivalent of 'rattling doorknobs' to see if easy access can be gained to a room." Pet. App. 2 n.1.

base of stolen information. Pet. App. 2-3; Gov't C.A. Br. 5-6.

In early 2002, petitioner designed a "brute force attack" program[2] to breach the UT computer system via a portal known as the "TXClass Learning Central: A Complete Training Resource for UT Faculty and Staff." TXClass was used by UT faculty and staff as a resource for continuing professional education of UT employees. Non-employee students such as petitioner were not authorized to use TXClass. Authorized users gained access to their TXClass accounts by typing their Social Security numbers in a field on the TXClass website's log-on page. Petitioner's "brute-force attack" program was designed to exploit the log-on protocol, automatically transmitting to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users. When the program hit a valid Social Security number in the TXClass database, it extracted personal information corresponding to that number and provided petitioner a "back door" into a larger UT database containing information about current and prospective UT students, employment applicants, and charitable donors. Over a fourteen-month period, petitioner obtained data on more than 45,000 current and prospective students, donors, and alumni. Pet. App. 3-4; Gov't C.A. Br. 7-8.

Petitioner's actions adversely affected the UT computer system, requiring UT to spend more than $122,000 to assess the damage and $60,000 to notify victims that their personal information and Social Security numbers

---

[2] "'Brute-force attack' is term of art in computer science used to describe a program designed to decode encrypted data by generating a large number of passwords." Pet. App. 3 n.2.

had been illegally obtained. Pet. App. 4; Gov't C.A. Br. 11.

UT contacted the Secret Service, and the ensuing investigation led to petitioner. Thereafter, petitioner admitted that he had created the brute-force attack program to obtain personal information from the UT system, but he disavowed that he intended to use or sell it. Pet. App. 4; Gov't C.A. Br. 10.

2. A federal grand jury in the Western District of Texas returned a four-count indictment charging petitioner with intentionally accessing a protected computer without authorization and recklessly causing damage, in violation of 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004) (Count 1), fraud in connection with access devices, in violation of 18 U.S.C. 1029(a)(3) (Counts 2 and 3), and fraud in connection with authentication features, in violation of 18 U.S.C. 1028(a)(6) (Supp. IV 2004) (Count 4). Pet. App. 4; Gov't C.A. Br. 3. Petitioner was tried before a jury. Pet. App. 4. At the close of the evidence, the district court provided the jury with the following instruction concerning Count 1:

> Title 18, United States Code, Section 1030(a)(5) makes it a Federal crime or offense for anyone, through means of a computer used in interstate commerce or communications, to knowingly and without authorization, cause the transmission of any program, code or command to another computer or computer system and recklessly causes damage to [the] receiving computer, computer system, network, information, data or program, or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program.

[Petitioner] can be found guilty of that offense only if all of the following facts are proved beyond a reasonable doubt:

First: That [petitioner], through means of a computer used in interstate commerce or communications, knowingly caused the transmission of a program, information, code or command to another computer or computer system, as charged;

Second: That [petitioner], by causing the transmission, acted with reckless disregard of a substantial and unjustifiable risk that the transmission would damage the receiving computer, computer system, information, data or program[,] or withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system or network, information, data or program;

Third: That [petitioner] so acted without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code or command; and

Fourth: That [petitioner's] acts caused loss or damage to one or more other persons of value aggregating $5,000 or more during any one year period.

Gov't C.A. Br. 25-26 (quoting charge).[3] Petitioner did not object to that instruction.

The jury convicted petitioner on Counts 1 and 4, and acquitted him on Counts 2 and 3. Petitioner timely filed a post-verdict motion for judgment of acquittal challenging the sufficiency of the evidence regarding the loss amount used to support his conviction on Count 1, and asserting that his conviction on Count 4 violated the Ex Post Facto Clause. Pet. App. 4-5. The district court denied the motion with respect to Count 1, but it granted the motion with respect to Count 4. *Id.* at 5 & n.3.

3. On appeal, petitioner contended, for the first time, that the jury instructions constructively amended the indictment by permitting the jury to convict him for violating Section 1030(a)(5)(A)(i)—*viz.*, knowingly causing the transmission of a program to a protected computer—when the indictment had only alleged a violation of Section 1030(a)(5)(A)(ii)—*viz.*, intentionally accessing a protected computer. Pet. App. 5-10. He further alleged that the deviation between the terms of the charged offense and the offense submitted to the jury warranted reversal of his conviction for two separate reasons. First, he alleged that the jury instruction failed to require the jury to find that he intentionally accessed TXClass without authorization, but instead only required that he transmitted a program without authorization. *Ibid.*; Pet. C.A. Br. 21. Second,

---

[3] As there was no pattern jury instruction for the Fifth Circuit with respect to this offense, the district court's charge was based on the government's proposed instruction, which was derived from the text of Section 1030(a)(5), 18 U.S.C. 1030(a)(5) (2000 & Supp. IV 2004), and a modified version of Eleventh Circuit Criminal Pattern Jury Offense Instruction 42.3 (2003). See Pet. App. 10; Gov't C.A. Br. 25.

he alleged that, while the charged offense, Section 1030(a)(5)(A)(ii), requires the government to prove that he "intentionally" accessed a protected computer without authorization, the jury instruction did not require the jury to find that he acted intentionally with respect to the lack of authorization. Pet. C.A. Br. 21-22. Petitioner conceded that he "did not object to the charge," *id.* at 20, and therefore that "[t]he standard of review is * * * plain error," *ibid.*, but he maintained that the asserted "constructive amendment" of the indictment qualified as reversible plain error, *id.* at 22-23.

The court of appeals affirmed. The court agreed with petitioner's concession that plain-error review applied because he failed to object below. Pet. App. 10. To prevail under that standard, petitioner must show that (1) there was error; (2) the error was plain; (3) the error affected his substantial rights; and (4) the error seriously affected the fairness, integrity, or public reputation of judicial proceedings. See *Johnson* v. *United States*, 520 U.S. 461, 466-467 (1997). Applying that standard to petitioner's first assertion, the court found that the jury instruction had plainly modified an essential element of the charged offense by "supporting the act of accessing a protected computer under subsection (ii) on the basis of transmitting a program under subsection (i)." Pet. App. 11. Nonetheless, the court found "no reversible plain error with respect to the transmission/access discrepancy" because there was "no conceivable basis upon which the jury could have concluded that [petitioner] transmitted the program and obtained information from UT's database without having also accessed a protected computer." *Id.* at 12. Accordingly, the instruction on that element of the offense, "although incorrect, was immaterial." *Ibid.*

The court of appeals also concluded that petitioner's second claim did not warrant reversal. The court agreed with petitioner that "the actus reus was the *intentional* unauthorized access of a protected computer." Pet. App. 12. But while the jury instruction did not explicitly require the jury to find "that [petitioner] intentionally acted without authorization," *id.* at 13, the court concluded that the evidence "leaves no doubt that [petitioner] knew he was unauthorized to transmit an invasive computer program designed to gain access to the TXClass system and to steal thousands of Social Security numbers," *ibid.* The court further explained: "It beggars belief that, having transmitted such a program, [petitioner] did not intend to access a protected computer and that he [sic] access be unauthorized." *Ibid.* Therefore, the court concluded that, "[t]o the extent the jury instructions were wrong, the errors did not affect [petitioner's] substantial rights." *Id.* at 13-14.[4]

ARGUMENT

Petitioner contends (Pet. 7-15) that the district court committed reversible plain error by instructing the jury concerning the "transmi[tting]" prong of 18 U.S.C. 1030(a)(5) (2000 & Supp. IV 2004) when the indictment alleged that petitioner had violated the "access[ing]"

---

[4] The court of appeals also rejected petitioner's argument, raised for the first time on appeal, that there was insufficient evidence that petitioner "intentionaly access[ed] a protected computer without authorization." Pet. App. 5 (quoting 18 U.S.C. 1030(a)(5)(A)(ii) (Supp. IV 2004)). After observing that petitioner was "never authorized to access TXClass," *id.* at 10, and that he "intentionally and meticulously executed both his intrusion into TXClass and the extraction of a sizable quantity of confidential personal data," *id.* at 8, the court concluded that "[t]here was no lack of evidence to find him guilty of intentional unauthorized access," *ibid.*

prong. Under the plain-error standard, a defendant is entitled to relief for an error to which he did not object at trial only if he can show that (1) there was error; (2) the error was plain; and (3) the error affected his substantial rights. If those three conditions are met, an appellate court may then exercise its discretion to notice a forfeited error, but only if the error (4) seriously affected the fairness, integrity, or public reputation of judicial proceedings. *Johnson* v. *United States*, 520 U.S. 461, 466-467 (1997); accord *United States* v. *Cotton*, 535 U.S. 625, 631-632 (2002). The court of appeals' conclusion that petitioner failed to satisfy the plain-error standard was correct, and petitioner identifies no circuit conflict on the application of that standard that warrants this Court's review. Indeed, this Court denied a petition for a writ of certiorari in another case raising a similar question concerning the application of the plain-error standard to constructive amendments, see *Murphy* v. *United States*, 546 U.S. 1097 (2006) (No. 05-6311),[5] and there is no reason for a different result in this case.

1. The Fifth Amendment's Grand Jury Clause states that "[n]o person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury." This Court has repeatedly held that the Grand Jury Clause requires that every element of a criminal offense be charged in a federal indictment. See, *e.g.*, *Almendarez-Torres* v. *United States*, 523 U.S. 224, 228 (1998); *United States* v. *Miller*,

---

[5] On June 20, 2007, the United States filed a brief in opposition to the petition for a writ of certiorari filed in *Pryor* v. *United States*, petition for cert. pending, No. 06-10280 (filed Mar. 23, 2007), which raises the same issue concerning the application of the plain-error standard to a constructive amendment claim.

471 U.S. 130, 136 (1985); *Hamling* v. *United States*, 418 U.S. 87, 117 (1974).

Petitioner contends (Pet. 6-15) that, by instructing the jury that it could convict if it found that the government had proven that petitioner knowingly transmitted a program, in violation of 18 U.S.C. 1030(a)(5)(A)(i), when the indictment alleged that petitioner had intentionally accessed a protected computer, in violation of 18 U.S.C. 1030(a)(5)(A)(ii), the district court permitted a "constructive amendment" of the indictment. See, *e.g.*, *Stirone* v. *United States*, 361 U.S. 212, 219 (1960) (reversing a verdict that may have rested on a factual theory different from that charged in the indictment on the ground that it was impossible to "know whether the grand jury would have included in its indictment a charge" based on that theory). Petitioner further contends that such a "constructive amendment" constitutes structural error, and thus automatically affects his substantial rights for purposes of the third prong of the plain-error standard. Pet. 6-10.

As a preliminary matter, not all deviations between the theory of guilt specified in the indictment and the government's evidence at trial constitute "constructive amendments." Where the divergence does not substantially alter the charged theory of guilt, lower courts have characterized it as a mere "variance" from the indictment, and have held that it affords no ground for reversal unless the divergence "is likely to have caused surprise or otherwise been prejudicial to the defense." 4 Wayne R. LaFave et al., *Criminal Procedure* § 19.6(c) at 808-809 & n.23 (2d ed. 1999) (citing cases). Only where the divergence sets an entirely new basis for conviction before the jury have lower courts characterized the divergence as a "constructive amendment" of the

indictment and generally held that it constitutes structural error (thereby requiring automatic reversal when an objection has been properly preserved). See *id.* § 19.6(c), at 811-812.

There is a substantial question whether the lower court decisions holding that a "constructive amendment" constitutes structural error remain valid in light of this Court's decisions holding that most constitutional errors are subject to harmless-error review. To the extent that lower courts have so held, cf. Pet. 8-10 (citing cases arising on plain-error review), those courts (like petitioner, see Pet. 6-10) have relied principally on this Court's decision in *Stirone*, which held that automatic reversal was warranted when the government proved an element at trial based on a factual theory that deviated from the factual theory advanced in the indictment and the defendant had raised a timely objection at trial. 361 U.S. at 217. *Stirone*, however, was decided before this Court held that harmless-error analysis was generally applicable to constitutional errors, see *Chapman* v. *California*, 386 U.S. 18, 22 (1967), and that harmless-error analysis was specifically applicable to the omission of an element of the offense from the jury's instructions, see *Neder* v. *United States*, 527 U.S. 1, 8-15 (1999).

2. Petitioner asserts (Pet. 10) that this Court's review is warranted to resolve a disagreement among the courts of appeals on whether errors of the sort at issue here constitute "structural errors" that necessarily affect petitioner's substantial rights for purposes of the third prong of the plain-error standard. Further review of that question is not warranted because, even if petitioner is correct that a constructive amendment is a structural error, he still would not be entitled to relief unless he could also satisfy the prerequisite for noticing

forfeited claims under the *fourth* prong of the plain-error standard: *i.e.*, by showing that the error seriously affected the fairness, integrity, or public reputation of judicial proceedings. Because petitioner cannot satisfy that prong, further review of the court of appeals' application of the third prong in this case is unwarranted.

Petitioner notes (Pet. 7-8) that, in *United States* v. *Floresca*, 38 F.3d 706 (1994) (en banc), the Fourth Circuit held that the "constructive amendment" of an indictment requires automatic reversal, even where an objection has not been properly preserved (and plain-error review is thus applicable). See *id.* at 714.[6] To the extent petitioner contends that this Court should adopt that rule, however, his contention is flawed. As petitioner tacitly recognizes (Pet. 11-13), *Floresca*'s reasoning has been called into question by this Court's intervening decision in *United States* v. *Cotton*, *supra*.

In *Cotton*, the district court sentenced the defendants to terms of imprisonment that exceeded the statutory maximum sentence that would have applied to the charge set out in the indictment. The Fourth Circuit reversed. *United States* v. *Cotton*, 261 F.3d 397, 404-407 (2001), rev'd, 535 U.S. 625 (2002). Relying on *Floresca*, it held that "sentencing a defendant for an unindicted crime" undermines the fairness, integrity, and public

---

[6] Although petitioner also (Pet. 6) cites *United States* v. *Thomas*, 274 F.3d 655 (2d Cir. 2001) (en banc), for the proposition that a "constructive amendment" automatically affects a defendant's substantial rights under the third prong of the plain-error test, the case—as petitioner himself recognizes (Pet. 7)—does not support the more ambitious proposition embraced by the Fourth Circuit, that a "constructive amendment" of an indictment *always* seriously affects the fairness, integrity, or public reputation of judicial proceedings (and thus requires automatic reversal even on plain-error review).

reputation of judicial proceedings in the same way that "convicting a defendant of an unindicted crime" does. *Id.* at 406 (emphasis omitted) (quoting *Floresca*, 38 F.3d at 714). This Court, however, reversed the court of appeals. It held that the defendants were not entitled to relief under the fourth prong of the plain-error standard because the evidence of the relevant sentence-enhancing fact that was not submitted to the jury (or charged in the indictment) was "overwhelming" and "essentially uncontroverted." *Cotton*, 535 U.S. at 633 (quoting *Johnson*, 520 U.S. at 470). The Court added that "[t]he real threat * * * to the 'fairness, integrity, and public reputation of judicial proceedings' would be if [the defendants], despite the overwhelming and uncontroverted evidence," were to receive a lesser sentence for a "less substantial" crime "because of an error that was never objected to at trial." *Id.* at 634.

In light of this Court's decision in *Cotton*, the Fourth Circuit's holding in *Floresca*—that the "constructive amendment" of an indictment requires automatic reversal even where an objection has not been properly preserved—should no longer be considered good law. The Fourth Circuit has not addressed the rule of *Floresca* since *Cotton*, and this Court has denied review in at least one case in which the petitioner alleged a circuit conflict with *Floresca*. See *United States* v. *Murphy*, 406 F.3d 857 (7th Cir. 2005), cert. denied, 546 U.S. 1097 (2006) (No. 05-6311). At a minimum, the Fourth Circuit should be permitted to reconsider the *Floresca* approach in an appropriate case before this Court intervenes. Indeed, as petitioner himself notes (Pet. 11-12), the Tenth Circuit has done precisely that and concluded that its pre-*Cotton* automatic reversal rule "no longer applies in a constructive amendment plain error case" in the wake of

Cotton. *United States* v. *Brown*, 400 F.3d 1242, 1253 n.6 (2005).

3. In the alternative, petitioner contends (Pet. 13-14) that, even if *Floresca* is no longer good law, the fourth prong of the plain-error standard is satisfied here because the evidence that he intentionally accessed the UT computer system without authorization was not "overwhelming" or "essentially uncontroverted." *Cotton*, 535 U.S. at 633 (quoting *Johnson*, 520 U.S. at 470). That fact-bound contention lacks merit and in any event does not warrant further review.

As the court of appeals concluded, the factual predicate for the transmission and access offenses—petitioner's use of the "brute-force attack program" to gain access to TXClass—was "identical," Pet. App. 12, and, therefore, there is "no conceivable basis upon which the jury could have concluded that [petitioner] transmitted the program and also obtained information from UT's database without having also accessed a protected computer." *Ibid.* Accordingly, while the district court erred in instructing the jury concerning transmission, the error was "immaterial," *ibid.*, because the jury's "transmission" finding necessarily included an "access" finding as well.[7] Moreover, the evidence that petitioner intentionally accessed TXClass without authorization was overwhelming. As the court of appeals observed, peti-

---

[7] Petitioner contends (Pet. 14) that he "did not 'transmit' any 'program.'" Regardless of whether he transmitted a "program," however, he clearly used the "brute-force attack program" to transmit social security numbers to the TXClass website in order to gain access to UT's database and extract information. The jury instructions permitted a finding of guilt based on the transmission not only of programs, but also of "information, code or command." See p. 5, *supra*. The social security numbers were "information" that petitioner transmitted.

tioner's "brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user." *Id.* at 8. To the contrary, petitioner "intentionally and meticulously executed both his intrusion into TXClass and the extraction of a sizable quantity of confidential personal data." *Ibid.*

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

PAUL D. CLEMENT
Solicitor General

ALICE S. FISHER
Assistant Attorney General

MICHAEL A. ROTKER
Attorney

AUGUST 2007